Remarks

The Official Action rejected claims 1-20. Applicant has amended claims 12-19. Applicant respectfully requests reconsideration in view of the present claim amendments and remarks.

Claim Rejections Under 35 USC § 101

The Official Action rejected claims 11-17 and 19-20 under 35 USC 101 because such claims are not limited to tangible embodiments. However, Applicant disagrees with the Official Actions assessment that signal transmissions such as optical, electrical, or air waves are intangible and are not statutory subject matter. In support of this proposition, one merely need to look to a microwave oven for evidence that signal transmissions (e.g. microwaves) do produce "tangible" results (e.g. heat food).

Further, Applicant respectfully submits that the Official Action has provided no basis for maintaining such a rejection beyond a blanket reference to 35 USC 101 and an indication that the identified claims encompass intangible embodiments. Applicant respectfully points out that the Supreme Court has held, Congress chose the expansive language of 35 U.S.C. 101 so as to include "anything under the sun that is made by man." Diamond v. Chakrabarty, 447 U.S. 303, 308-09, 206 USPQ 193, 197 (1980). The Applicant respectfully points out that signal transmission embodiments of claims 11-17 and 19-20 are "made by man". Further, such signal transmissions embodiments encompassed by claims 11-17 and 19-20 are not naturally occurring phenomena nor do such signal transmission embodiments appear to fall within other judicially created exceptions.

Applicant respectfully requests the rejection of claims 11-17 and 19-20 under 35 USC 101 be withdrawn. If the Examiner elects to maintain the present rejection of claims 11-17 and 19-20 under 35 USC 101, Applicant requests the Examiner to provide a more detailed explanation why such claims are not deemed statutory subject matter. Such an explanation should include references to legal precedents and application of such legal precedents to the claims at issue.

Claim Rejections Under 35 USC § 102

The Official Action rejected claims 1-20 under 35 U.S.C. 102(e) as being anticipated by Davis et al. (US Patent No. 6,401,208). Applicant has amended claims 12-19 and respectfully requests reconsideration.

As is well-established, in order to successfully assert a *prima facie* case of anticipation, the Official Action must provide a single prior art document that includes every element and limitation of the claim or claims being rejected. Therefore, if even one element or limitation is missing from the cited document, the Official Action has not succeeded in making a prima facie case.

Claims 1 and 11

Claim 1 is directed to a code module comprising code and a signature encrypted such that a computing device is capable of decrypting the signature using ***a key embedded in a chipset*** of the computing device. Claim 11, however, is directed to a machine readable medium comprising code pages and a value encrypted such that a computing device is capable of decrypting the value using ***a key embedded in a processor*** of the computing device. The Official Action appears to have overlooked the limitation "a key embedded in a chipset" of claim 1 and "a key embedded in a processor" of claim 11 which effect the manner the

signature of claim 1 and the machine of claims 1 and the value of claim 11 are generated such to permit decryption with embedded keys of the chipset and processor respectively.

The Official Action grouped these two claims together and cited column 3, lines 6-40 of Davis to support anticipation of claims 1 and 11. Davis in the cited column teaches a storage device 170 that contains BIOS code 180 and a digital BIOS certificate 181 and a BIOS signature 182. Davis further teaches that the BIOS signature 182 includes a digest of the BIOS code 180 signed by a private key of the BIOS vendor and that the BIOS certificate 181 includes a public key of the BIOS vendor signed by a private key of a certification authority. Davis however in column 3, lines 6-40 does not indicate how the digest of the BIOS signature 182 is decrypted and thus does not teach in the cited column 3, lines 6-40 a signature capable of being decrypted by an embedded key of a chipset (claim 1) or a value capable of being decrypted by an embedded key of a processor (claim 11).

While the cited section of Davis does not teach how the digest of the BIOS signature is decrypted, other sections of Davis provide such information. In particular, Davis teaches pre-programming a cryptographic device 410 with a root certificate key 527. Davis column 5, lines 9-13. The cryptographic device 410 decrypts the BIOS certificate 181 using the root certificate key 527 of the cryptographic device 410 to obtain the public key of the signatory (e.g. BIOS vendor) of the BIOS signature 182. The cryptographic device 410 then uses the public key obtained from the BIOS certificate 181 to decrypt the digest of the BIOS signature 182. In sum, Davis appears to teach a storage device 170 that stores BIOS code 180, a BIOS certificate 181, and a BIOS signature 182 that is capable of being

decrypted using ***a key of the BIOS certificate 181 stored in the storage device 170***.

Since Davis does not appear to teach a signature capable of being decrypted using a key of a chipset (claim 1) or a value capable of being decrypted using a key of a processor (claim 11), Davies does not anticipate the invention of claim 1 or the invention of claim 11. Accordingly, Applicant respectfully requests the rejection of claim 1 and the rejection of claim 11 be withdrawn.

Claim 19

Claim 19 as amended is directed to machine readable medium comprising data pages, code pages, and a value encrypted such that a computing device is capable of decrypting the value ***using an asymmetric key embedded in a chipset*** of the computing device. As mentioned above, Davis does not appear to teach a value capable of being decrypted using an key embedded in a chipset. Accordingly, Davis does not appear to anticipate the invention of claim 19. Applicant respectfully requests the rejection of claim 19 be withdrawn.

Claims 4,13 and 20

Each of claims 4, 13 and 20 includes a ***SHA-1 hash*** limitation. While Davis may disclose using a one-way hash, Applicant has been unable to locate where Davis teaches specifically using a SHA-1 hash as required by claims 4, 13 and 20. Without such a teaching, Davis does not anticipate the invention of claims 4, 13 and 20. Applicant respectfully requests the rejection of claims 4, 13 and 20 be withdrawn.

Claims 6 and 14

Each of claims 6 and 14 require a field that identifies/specifies an execution point from which a computing device executes code. The Official Action relies on column 4, lines 41-59 of Davis for such a teaching. As far as the Applicant can determine, Davis at column 4, lines 41-59 merely teaches that internal memory 525 contains firmware 526 which is a small computer program executed by first IC device 500. Column 4, lines 41-59 appears to provide no teaching regarding at what point or location execution of the firmware is to begin. Accordingly, Davis does not appear to teach a code module or a machine readable medium that has a field to identify/specify an execution point from which a computing device executes code. Applicant respectfully requests the present rejection of claims 6 and 14 be withdrawn.

Claims 7 and 15

Each of claims 7 and 15 require a marker that specifies the end of the code module (claim 7) or that specifies the end of the code pages and data pages (claim 15). The Official Action relies on column 6, lines 20-30 of Davies for such a teaching. Davis, however, at column 6, lines 20-30 appears to be silent in regard to a marker of a code module or a machine readable medium (See, FIG. 2 of Applicant's application) that specifies the end of a code module or the end of code pages and data pages. Davis in the specified section appears to teach generating a soft reset once BIOS code has been authenticated and to begin execution at a standard reset vector in response to the soft reset. Applicant respectfully requests the present rejection of claims 7 and 15 be withdrawn.

Claims 8 and 16

Each of claims 8 and 16 require one or more fields that specify an encryption algorithm used to encrypt the signature and that specify an algorithm used to compute the digest value. Such fields enable code modules and machine readable medium to use different types of encryption algorithms and digest algorithms since the computing device may refer to these fields to determine appropriate algorithms to use in order to decrypt the signature and to validate the digest value. The Official Action relies on column 2, lines 53-56 for such a teaching. Column 2, lines 53-56 merely provides a definition of a digital signature. There appears to be no teaching in Davis at the cited location or elsewhere regarding fields of a code module or a machine readable medium that specifying an encryption algorithm used to encrypt the signature and that specify an algorithm used to compute the digest value. Applicant respectfully requests the present rejection be withdrawn.

Claims 2, 3, 5, 9, 10, 12, 17 and 18

Each of claims 2, 3, 5, 9, 10, 12, 17 and 18 depends from one of claims 1 and 11. Accordingly, each of claims 2, 3, 5, 9, 10, 12, 17 and 18 is allowable for at least reasons stated above in regard to claims 1 and 11.

Conclusion

Additional points could be made to distinguish claims 1-20 from Davis. However, Applicant believes the rejection has been overcome in light of the above. Applicant therefore elects to reserve such points so as to not burden the Examiner with superfluous points at this time.

The foregoing is submitted as a full and complete response to the Official Action. Applicant submits that all remaining claims are in condition for allowance. Reconsideration is requested, and allowance of all remaining claims is earnestly solicited.

Should it be determined that an additional fee is due under 37 CFR §§1.16 or 1.17, or any excess fee has been received, please charge that fee or credit the amount of overcharge to deposit account #02-2666. If the Examiner believes that there are any informalities which can be corrected by an Examiner's amendment, a telephone call to the undersigned at (503) 439-8778 is respectfully solicited.

Respectfully submitted,

Paul Mendonsa
Reg. No. 42,879

Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1030
(408) 720-8300